ABSTRACT

~~A method and an embedded system for verifying a request to certify a public key (Kp) generated by an embedded system with the identifier (SN$_i$).~~

For a set (Lk) of embedded systems, an authorized operator with ~~the~~ identifier (OP$_j$) ~~configures the embedded systems and~~ creates ~~(1001)~~ a mother public key (KpM) and a mother private key (KsM). The identifier (OP$_j$), the range of identifiers referenced (Lk) and the mother public key (KpM) are published ~~(1002)~~. For each embedded system (SN$_i$), a diversified key (KsM$_i$) is created from the identifier (SN$_i$) and stored ~~(1003)~~ ~~in read- and write-protected storage~~. For every public key (Kp) generated by an embedded system, a cryptographic control value (Sc$_i$) is calculated ~~(1006)~~ on the public key (Kp), an algorithm identifier (CA1) and the utilization parameters (U) of this key, using a zero knowledge signature algorithm, and a certification request message (MRCA) that includes ~~the~~ control value (Sc$_i$), the identifier of the operator (Op$_j$), and ~~the~~ identifier (SN$_i$) is transmitted to a certification authority, which retrieves the identifier (Op$_j$) ~~(1009)~~ and the value of the mother public key (KpM) ~~(1011)~~. ~~A verification (1012) of the message (MRCA) from the mother public key (KpM) and from the identifier of the embedded system (Sn$_i$) makes it possible to be sure that the request to certify a public key (Kp) and the utilization of the latter actually originates from an embedded component capable of limiting the use of this key.~~

~~Fig. 2a.~~